

OCT 08 2019

**AFFIDAVIT**AT BALTIMORE  
CLERK, U.S. DISTRICT COURT  
DISTRICT OF MARYLAND

I, JASON P. LEBEAU, being duly sworn on oath, depose and state as follows:

BY

DEPUTY

**INTRODUCTION**

A. I am a Special Agent with the Federal Deposit Insurance Corporation-Office of Inspector General (FDIC-OIG). I have been a Special Agent with FDIC-OIG from April 2014 until present, where my responsibilities include the investigations of various financial crimes of Title 18 of the United States Code, such as violations of bank fraud, wire fraud, mail fraud, and similar offenses. Prior to this employment, I was a Special Agent with IRS-Criminal Investigation from October 2001 until April 2014, where my responsibilities also included the investigation of financial crimes, such as criminal violations of the Internal Revenue Code, Title 26, United States Code (violations of tax law), Title 31, United States Code (violations of currency reporting requirements), and related offenses of Title 18, United States Code (including violations of money laundering). Throughout my career as a Special Agent, I have participated in numerous federal investigations involving bank fraud violations, wire fraud violations, financial reporting fraud violations, money laundering violations, and tax violations.

B. I am a Certified Public Accountant (CPA), a Certified Fraud Examiner (CFE), and a Certified Anti-Money Laundering Specialist (CAMS). Prior to becoming a Special Agent, I received a bachelor's degree in accounting in May 2001 and then briefly worked for a large public accounting firm in Chicago, Illinois. Subsequently, I received law enforcement training at the Federal Law Enforcement Training Center in Glynco, Georgia, graduating in December 2001 from the Criminal Investigator Training Program and graduating in March 2002 from the Special Agent Basic Training Program.

C. I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct investigations of, and to make arrests for, federal felony offenses. Here, I am one of the case agents investigating the alleged bank fraud and wire fraud committed by Lovette Namatinga (Namatinga) in connection with funds fraudulently obtained from various businesses as set forth in detail below. In my experience, I have learned that individuals normally maintain financial records, property records, and business records in their residence and place of business. It is also my experience that financial, property, and business records/files are maintained on computers, discs, thumb drives, detachable drives, and other electronic devices, which are maintained at residences and places of business.

D. This affidavit is made in support of an application for search warrants to search:

- a. the listed business premises of Keiko San Products Alimenticious, LLC (Keiko), which, according to Maryland Department of Assessment and Taxation filings, is located at 130 Persimmon Circle, Reisterstown, MD;
- b. the personal residence of Namatinga located at 10913 Huntcliff Drive, Apt. 9, Owings Mills, MD;
- c. Namatinga's mobile telephone, an Apple iPhone X with International Mobile station Equipment Identity number 354876091091293;
- d. Namatinga's vehicle, a 2015 Toyota Corolla with MD tag number 6BV6137; and,
- e. Namatinga's person, including any baggage in his possession.

which are further described in Attachments A1, A2, A3, A4, and A5. The search is for evidence and instrumentalities, which are described further in Attachments B1 and B2, concerning Namatinga's bank fraud in violation of Title 18, United States Code, Section 1344 and wire fraud

in violation of Title 18, United States Code, Section 1343. Agents of the FDIC-OIG have driven by and viewed the exteriors of both the listed business premises and the personal residence locations to be searched.

E. The statements contained in this affidavit are based, in part, on my own investigation, as well as on information provided to me by other law enforcement officers, on information provided by other witnesses, and on my own experience, training, and background as a Special Agent with both the Internal Revenue Service- Criminal Investigation and the Federal Deposit Insurance Corporation-Office of Inspector General. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge, or the knowledge of others, about this matter.

### **FACTUAL BACKGROUND**

#### **I. Namatinga's Immigration and Employment**

6. On or about June 22, 2012, Namatinga, a Cameroonian citizen, came to the United States on a Diversity Immigration Visa. Once immigrated to the United States, it is unknown how Namatinga was employed in the early years. Since 2016, the Maryland Department of Labor reports that Namatinga has been employed at Fawema Enterprises, a company that serves individuals with disabilities. Since 2018, the Maryland Department of Labor also reports that Namatinga has been employed at L.I.F.E., Inc., a non-profit agency dedicated to helping adults with special needs. In addition, from 2016 until 2018, the Maryland Department of Labor reports that Namatinga worked at Dominion Resource Center, a non-profit agency that provides opportunities for seniors and the mentally impaired.

## **II. Namatinga's Fraudulent Bank Activity Through Keiko San Products**

### **A. Keiko San Products Bank Accounts**

F. On or about October 27, 2018, Namatinga opened a business checking account, with account number 3619691326, in the name of Keiko San Products Alimenticios, LLC (Keiko), at a Wells Fargo Bank branch in Owings Mills, MD. According to the signature card, Keiko is located at 130 Persimmon Circle, Reisterstown, MD, and is purportedly owned by Namatinga and Abigail Dzanni (Dzanni), both of whom are reported to reside at 10913 Huntcliff Drive, Apt. 9, Owings Mills, MD. According to the Maryland Department of Assessments & Taxation, Namatinga is the registered agent of Keiko. The business industry of Keiko, as described on the Wells Fargo signature card, is food production and car services.

G. On or about September 10, 2018, approximately one month prior to the opening of the Wells Fargo account, account number 1000245828461 was opened in the name of Keiko at a SunTrust Bank branch in Owings Mills, MD. According to the SunTrust Bank records, the Keiko mailing address is 25 Enchanted Hills Rd, Apt. 1, Owings Mills, MD (differing from the address shown on the Wells Fargo records). SunTrust Bank records initially indicated that the owner, and only person listed on the initial signature card, was Sheriff A. Sofo (Sofo). On or about March 26, 2019, however, Namatinga was added as an authorized signer on the account, while Sofo remained the sole owner.

### **B. Attempted Fraudulent Transfer Through Fidelity Investments**

9. On or about November 29, 2018, a male contacted Fidelity Investments and purported to be a Fidelity customer. The caller was able to answer a series of knowledge-based questions and ultimately requested a disbursement of \$28,500 from the Fidelity customer's account. The caller requested that Fidelity send the check to Keiko and provided an address of

10913 Huntcliff Drive, Apt. 9, Owings Mills, MD (the address listed for Namatinga on the Wells Fargo signature card). The check was issued, subsequently endorsed by what appears to be Namatinga's signature, and on or about December 4, 2018, was deposited into the Keiko bank account at SunTrust Bank (8461). Fidelity eventually realized the transfer request was not conducted by the true customer and was able to stop payment on this check, even though the check had already been deposited into the Keiko account at SunTrust Bank (8461). I interviewed the true Fidelity customer and he confirmed that he did not authorize the transfer in question. Neither Fidelity nor SunTrust Bank suffered a loss due to this transaction.

C. Fraudulent Transfers Through Municipal Trust and Savings Bank

10. On or about February 26, 2019, Municipal Trust and Savings Bank (MTSB), which is located within the Central District of Illinois, received a series of emails from an individual who purported to be the secretary of one of their loan customers. The series of emails requested that MTSB mail a check in the amount of \$37,650.40 to Keiko at 10913 Huntcliff Drive, Apt. 9, Owings Mills MD, which is also Namatinga's home address. The funds were drawn from the MTSB customer's line of credit and the check was mailed as requested. On or about February 27, 2019, this check was deposited into the aforementioned Keiko account at Wells Fargo (1326) and the check appears to be endorsed by Namatinga. Wells Fargo video footage shows this transaction was conducted by an individual who appears to be Namatinga. On or about March 4, 2019, and March 7, 2019, funds in the amount of \$2,000 and \$1,000, respectively, were transferred from the Keiko account to a Wells Fargo checking account in the name of Namatinga (0993). On or about March 8, 2019, a withdrawal of \$32,500 was made from the Keiko account at Wells Fargo (1326) and a corresponding Currency Transaction Report (CTR) confirms the withdrawal was made in

cash. Wells Fargo video footage shows this transaction was conducted by an individual who appears to be Namatinga.

11. On or about March 11, 2019, MTSB received a second series of emails from an individual who again purported to be the secretary of the same loan customer. This time, the emails requested that MTSB mail another check in the amount of \$41,200.40 to Keiko. The funds were drawn from the MTSB customer's line of credit and the check was mailed to 10913 Huntcliff Drive, Apt. 9, Owings Mills MD. On or about March 13, 2019, this check was deposited into the Keiko account at Wells Fargo (1326) and the check appears to be endorsed by Namatinga. Wells Fargo video footage shows this transaction was conducted by an individual who appears to be Namatinga. On that same day, according to Immigration and Customs Enforcement (ICE) records, Namatinga flew to Germany (five days after withdrawing \$32,500 in cash from the Keiko account at Wells Fargo as described in Paragraph 10). Namatinga subsequently traveled to Lagos, Nigeria, where it appears that he stayed until his return to the United States on or about March 22, 2019. While Namatinga was apparently in Nigeria, ATM transactions were conducted through the Wells Fargo Keiko account (1326) at locations in Lagos, Nigeria. While Namatinga was outside the United States, an online transaction also was conducted on or about March 15, 2019 transferring \$4,000 from the Keiko account at Wells Fargo (1326) to Namatinga's personal savings account at Wells Fargo (9263). In addition to traveling back to the United States on or about March 22, 2019, an online transaction of \$36,000 was conducted on or about March 22, 2019, transferring funds from the Keiko account at Wells Fargo (1326) to Namatinga's personal Wells Fargo checking account (0993).

12. On or about March 23, 2019, approximately one day after returning to the United States and approximately one day after conducting the \$36,000 transfer from the Keiko account to

his personal checking account (0993), Wells Fargo records show two withdrawals from the checking account (0993) were conducted at two separate Wells Fargo branches in the amounts of \$20,000 and \$15,000. These withdrawals occurred at approximately 9:44 a.m. and approximately 10:16 a.m. A corresponding Currency Transaction Report (CTR) confirms that these transactions were both cash withdrawals. Wells Fargo video footage shows these transactions were conducted by an individual who appears to be Namatinga. The video footage also shows what appears to be Namatinga wearing a backpack during the second withdrawal. On or about March 25, 2019, an online transaction was conducted transferring \$3,000 from Namatinga's personal checking account at Wells Fargo (0993) to his personal savings account at Wells Fargo (9263).

13. On or about March 25, 2019, MTSB received a third series of emails from an individual who again purported to be the secretary of the same loan customer. This time, the emails requested that MTSB mail a check in the amount of \$40,506.70 to the same Keiko address, which is Namatinga's home address. The funds were drawn from the MTSB customer's line of credit and the check was mailed. On or about March 26, 2019 the check, this time endorsed by what appears to be Sofu's signature, was deposited into the Keiko account at SunTrust Bank (8461). On or about that same day, as previously mentioned, Namatinga was added to the Keiko account at SunTrust Bank as an authorized signer. Numerous cash withdrawals were conducted from this account following the deposit of this MTSB check, as shown below<sup>1</sup>:

- On or about April 1, 2019: \$500 (ATM)
- On or about April 1, 2019: \$500 (ATM)
- On or about April 3, 2019: \$8,000 (Signature appears to be that of Sofu)

---

<sup>1</sup> It should be noted that in addition to the MTSB deposit of \$40,506.70 on March 25, 2019, a deposit of \$17,000 was deposited into the account on April 15, 2019, for a purported car sale. The check was drawn on a Discover account.

- On or about April 3, 2019: \$5,000 (Signature appears to be that of Sofo)
- On or about April 4, 2019: \$500 (ATM)
- On or about April 4, 2019: \$500 (ATM)
- On or about April 4, 2019: \$10,000 (Signature appears to be that of Sofo)
- On or about April 4, 2019: \$5,000 (Signature appears to be that of Sofo)
- On or about April 5, 2019: \$500 (ATM)
- On or about April 5, 2019: \$500 (ATM)
- On or about April 5, 2019: \$6,500 (Signature appears to be that of Sofo)
- On or about April 8, 2019: \$500 (ATM)
- On or about April 8, 2019: \$500 (ATM)
- On or about April 17, 2019: \$700 (Signature appears to be that of Namatinga)
- On or about April 18, 2019: \$1,000 (Signature appears to be that of Namatinga)
- On or about April 22, 2019: \$2,000 (Signature appears to be that of Namatinga)
- On or about April 23, 2019: \$10,000 (Signature appears to be that of Namatinga)
- On or about April 23, 2019: \$4,000 (Signature appears to be that of Namatinga)
- On or about April 23, 2019: \$500 (ATM)
- On or about April 23, 2019: \$300 (ATM)

14. On or April 8, 2019, MTSB received a fourth series of emails from an individual who again purported to be the secretary of the same loan customer. This time, the emails asked for an update on the remaining balance within the customer's line of credit and requested that MTSB mail a check in the amount of \$21,650.70 to the same Keiko address, which is Namatinga's home address. The funds were drawn from the MTSB customer's line of credit and the check was mailed. On or about April 9, 2019, the check was deposited into the Keiko account at Wells Fargo



(1326) and the check appears to be endorsed by Namatinga. Wells Fargo video footage on April 9, 2019, shows this deposit was conducted through the Wells Fargo drive-through lane by someone in a dark colored Toyota Corolla. On or about April 12, 2019, funds in the amount of \$3,000 were transferred from the Keiko account at Wells Fargo (1326) to an individual Wells Fargo savings account in the name of Namatinga (9263). On or about April 18, 2019, Wells Fargo records indicate that a withdrawal in the amount of \$10,000 was conducted from the Keiko account at Wells Fargo (1326). Wells Fargo video footage shows this transaction was conducted by an individual who appears to be Namatinga.

15. On or about April 18, 2019, after MTSB realized that their customer had not made any of the draw requests described in Paragraphs 10 through 14 and recognized that it and the customer were victims of fraud;<sup>2</sup> MTSB placed a “stop payment” on the final check issued. MTSB reports a loss of approximately \$141,000 and Wells Fargo reports a loss of approximately \$14,000 as a result of these fraudulent transfers.

D. Fraudulent Transfers Through Anytickets.com

16. Unrelated to the transactions discussed above, on or about January 16, 2019, an entity entitled Events BSB Company, LLC (d/b/a Anytickets.com), located in Houston, Texas, received an email similar to the emails received by MTSB. The email requested that the Anytickets.com Controller wire \$23,955 to a JP Morgan Chase account in the name of Aida Knowles (Knowles). The funds were wired to the named account before it was realized that the email was fraudulent. On or about that same day, a cashier’s check drawn from Knowles’ JP Morgan Chase account was drafted in the amount of \$16,768.50. On or about January 18, 2019, this check was deposited into the Keiko account at Wells Fargo (1326). According to police

---

<sup>2</sup> This investigation confirmed that neither the MTSB loan customer nor his secretary sent the emails requesting the loan advances. The MTSB loan customer operates a realty company in Santa Monica, California.

reports filed by Anytickets.com, the customer has suffered a loss of the entire \$23,955 due to this fraud<sup>3</sup>.

E. Summary of Namatinga's Fraudulent Activity

17. From the October 2018 inception of the Keiko account at Wells Fargo (1326) until the final fraudulent deposit transacted in April 2019, approximately \$158,077 was deposited into the Keiko account owned by Namatinga. Approximately \$117,270 (or approximately 75 percent) of the total deposits were derived from fraudulent activity. Approximately \$28,611 (or approximately 18 percent) of the total deposits consisted of cash deposits.<sup>4</sup> Based on these facts, as well as my training and experience, it does not appear that normal business transactions were conducted through this business checking account, rather it primarily was used by Namatinga to process fraudulently obtained proceeds. Furthermore, as of May 22, 2019, Namatinga had not responded to email or voicemail requests for contact by Wells Fargo. According to Wells Fargo, Namatinga is not cooperating.

18. Based on the foregoing, your affiant alleges there is probable cause to believe that Namatinga has committed violations of Bank Fraud, in violation of Title 18, United States Code, Section 1344 and violations of Wire Fraud, in violation of Title 18, United States Code, Section 1343.

---

<sup>3</sup> Anytickets.com also reported a loss of \$98,550 regarding a similar fraudulent email requesting a transfer to an entity called Huanyu Fu Trading Co. Limited in Hong Kong.

<sup>4</sup> According to Weis Market, a supermarket that offers money wire services, Namatinga conducted approximately 18 wire transfers totaling approximately \$8,595.72 to various individuals located in Ghana and Cameroon between August 25, 2018 and December 1, 2018. According to Money Gram, he also conducted approximately 48 wire transfers totaling approximately \$8,034 to various individuals located in Cameroon, Thailand, and Italy between January 2, 2017 and May 22, 2017.

F. Namatinga's Plans to Leave the United States

19. According information obtained from U.S. Customs and Border Patrol, Namatinga has purchased international airline tickets and is scheduled to depart from Dulles International Airport, on October 7, 2019, at 6:05 p.m. on Air France Flight 55 to Paris, France.

20. Based on Namatinga's activities uncovered in the course of this investigation, and my training, knowledge, and experience with international bank and wire fraud conspiracies, I submit there is probable cause to believe that evidence of the offenses will also be located on his person and in any of his checked or carry-on baggage.

**APPLICATION**

**I. Premises Located at 10913 Huntcliff Drive, Apartment 9, Owings Mills, MD and 130 Persimmon Circle, Reisterstown, MD**

21. According to the Maryland Department of Assessments & Taxation, Namatinga is the registered agent for Keiko. His personal address is listed as 10913 Huntcliff Drive, Apt #9, Owings Mills, MD. Per the registration filings, the principal office of business of Keiko has been consistently listed as 130 Persimmon Circle, Reisterstown, MD.

22. According to Wells Fargo records, Namatinga opened a personal checking account and a personal savings account on or about August 16, 2018. The signature cards for these accounts both list Namatinga's mailing address as 10913 Huntcliff Dr., Apt 9, Owings Mills, MD. Furthermore, on or about October 27, 2018, the Keiko checking account was opened at Wells Fargo—Namatinga is the only authorized signer on that account. The signature card for the Keiko account lists the mailing address as 130 Persimmon Cir, Reisterstown, MD and lists the owner/key individuals of this account as Namatinga and Abigail Dzanni who, according to the signature card, reside at 10913 Huntcliff Dr., Apt 9, Owings Mills, MD. Funds from the scheme described in the

Factual Background section above were transferred between all three of these accounts, with which the premises are connected.

23. On or about November 29, 2018, a male caller contacted Fidelity and requested the mailing of a check—a request later determined to be fraudulent—to 10913 Huntcliff Drive, Apt. 9, Owings Mills, MD, which is Namatinga’s mailing address. Moreover, beginning on or about February 26, 2019, and continuing until on or about April 8, 2019, fraudulent requests were made to send checks from MTSB to 10913 Huntcliff Drive, Apt. 9, Owings Mills, MD—Namatinga’s home address. Based on my training and experience, I know that people tend to store financial records in a safe location such as their home or place of business.

## **II. Namatinga’s Mobile Telephone**

24. On or about September 3, 2019, T-Mobile provided records indicating that Namatinga is the subscriber of telephone number 202-751-6390. The subscriber effective date reported by T-Mobile was October 17, 2015. As of September 3, 2019, the account remains active and the “bill address” is listed as 10913 Huntcliss Dr., Apt 9, Owings Mills, MD. I believe the listing of “Huntcliss” to be a scrivener’s error that should state “Huntcliff”.

25. The International Mobile station Equipment Identity number (IMEI) is a number used to identify a device that uses terrestrial cellular networks. T-Mobile reports the IMEI for Namatinga’s phone as 354876091091293. IMEI.info is a website that allows for research of IMEI numbers to determine information about the device using the IMEI. According to IMEI.info, the IMEI reported by T-Mobile is used on an Apple iPhone X with iOS (iPhone Operating System).

26. According to Wells Fargo records, from at least February 26, 2019, through at least April 8, 2019 (during the time of the fraudulent transfers through MTSB described in the Factual Background section above) the Keiko Wells Fargo account was accessed almost exclusively by an

iPhone mobile device with an iPhone Operating System. In addition, in March 2019, when Namatinga is believed to have been in Nigeria, access to the Keiko Wells Fargo account occurred from an IP address in Nigeria using an iPhone mobile device with an iPhone Operating System. On several occasions, Wells Fargo video footage shows what appears to be Namatinga using a mobile telephone while conducting various transactions. Based on my training and experience, I am aware that most people keep their mobile telephones on their person or in their residence when not in use.

### **III. Namatinga's Vehicle**

27. According to vehicle registration records, a 2015 Toyota Corolla with MD tag number 6BV6137 is registered to Namatinga. This vehicle was seen by investigating agents near the entrance of 10913 Huntcliff Drive, Apt. 9, Owings Mills, MD—Namatinga's apartment building—as recently as August 8 and August 9, 2019.

28. Furthermore, on August 1, 2019, Wells Fargo Financial Crimes Investigator Ryan Smith provided a picture of the vehicle that went through the Wells Fargo drive-through lane on April 9, 2019, to make a deposit of the fraudulent MTSB check in the amount of \$21,650.70. According to Smith, the vehicle is a dark colored Toyota Corolla, but the license plate was unreadable. I have concluded that the car appears to be the same Toyota Corolla registered to Namatinga that has been seen near 10913 Huntcliff Drive, Apt. 9, Owings Mill, MD on August 8 and August 9, 2019. Wells Fargo video footage also shows what appears to be Namatinga conducting transactions through drive-through lanes driving a dark colored vehicle on various other days as well.


#### **IV. Conclusion**

29. Based on the foregoing, I believe there is probable cause that on the premises located at 10913 Huntcliff Drive, Apt. 9, Owings Mills, MD and 130 Persimmon Circle, Reisterstown, MD, as more particularly described in Attachments A1 and A2, which are attached hereto and specifically incorporated herein by reference, items that constitute evidence of the commission of an offense in violation of Title 18, United States Code, Section 1344 (bank fraud) and Title 18, United States Code, Section 134 (wire fraud), that are contraband and/or fruits of crime, and that are intended for use or have been used as the means of committing a criminal offense, will be found. I also believe that there is probable cause that such contraband and/or fruits of crime, which are intended for use or have been used as the means of committing a criminal offense, will be found on Namatinga's mobile telephone with IMEI 354876091091293, as more particularly described in Attachment A3, and in his Toyota Corolla vehicle with MD tag number 6BV6137, as more particularly described in Attachment A4. Furthermore, I believe that there is probable cause that the items listed in Attachment B1 will be located on Namatinga's person and in any of his baggage, including items to be checked or carried on his flight, as more particularly described in Attachment A5. These items are more specifically described in Attachments A1, A2, A3, A4, and A5, and Attachments B1 and B2, which are attached hereto and specifically incorporated herein by reference.

19-3265 ADC

19-3269 ADC

FURTHER AFFIANT SAYETH NOT.

  
JASON P. LEBEAU  
Special Agent, Federal Deposit Insurance  
Corporation – Office of Inspector General

Subscribed and sworn to me before this 7<sup>th</sup> day of October, 2019.

  
A. David Copperthite  
United States Magistrate Judge

**ATTACHMENT A1**

**Description of Premises to be Searched**

The property located at 130 Persimmon Circle, Reisterstown, MD, is a two-story townhouse.

The property has tan-colored siding and sits above a garage door. A set of stairs approaches a dark-colored door with the numbers 130 directly next to the door. This warrant authorizes the search of the residence, the garage, and any outbuildings or appurtenances thereto.

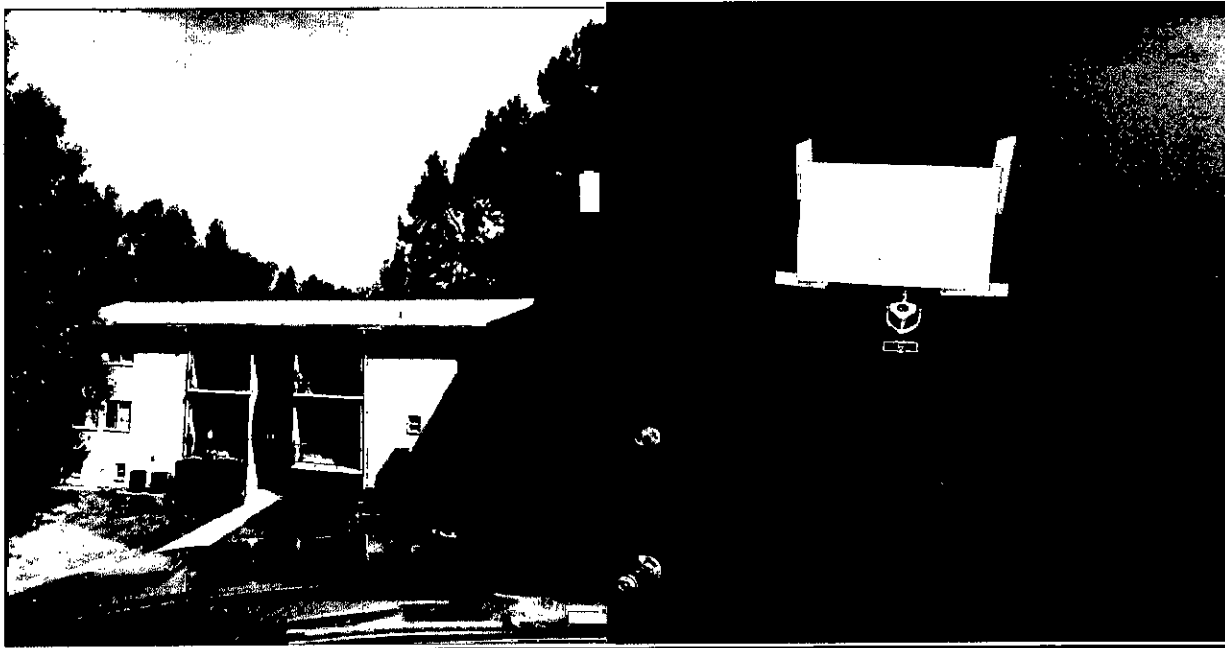




**ATTACHMENT A2**

**Description of Premises to be Searched**

The property located at 10913 Huntcliff Drive, Apartment 9, Owings Mills, MD, is located within an apartment building that contains three floors of apartments. The building is a brown-colored brick building with a green awning containing the numbers 10913. Apartment 9 is located on the top floor/back side of the building. The entry door to the apartment is green and contains the number 9 on the door.



**ATTACHMENT A3**

**Description of Premises to be Searched**

Apple iPhone X with International Mobile station Equipment Identity number (IMEI)

354876091091293.

**ATTACHMENT A4**

**Description of Premises to be Searched**

A dark colored Toyota Corolla bearing a Maryland license plate number 6BV6137



**ATTACHMENT A5**

**Description of Person and Items to be Searched**

The person of Lovette Namatinga, including any baggage in his possession:

Name: Lovette Namatinga

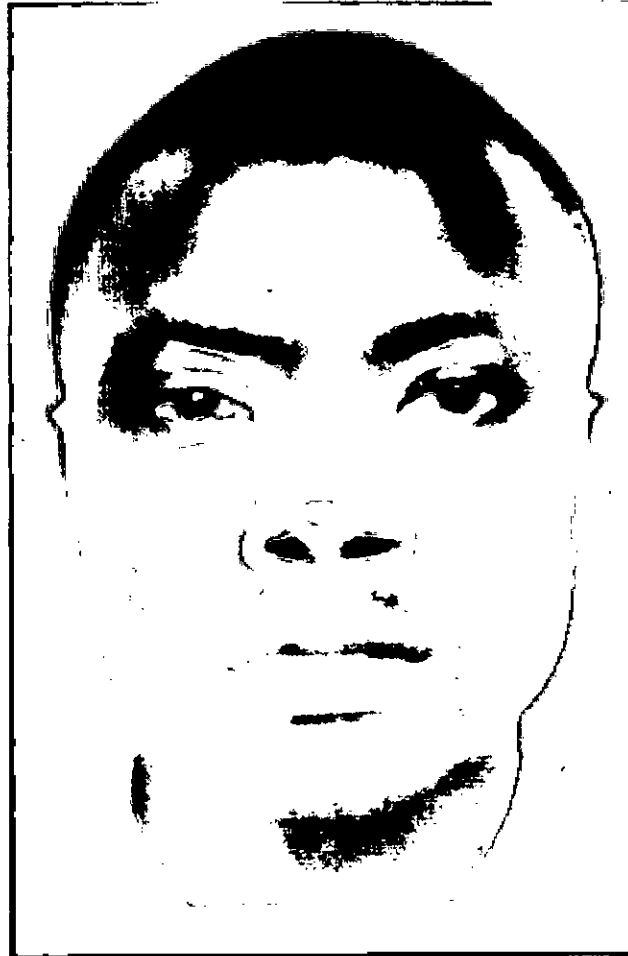
DOB: 3/3/1987

Sex: M

SSN: 728-81-0010

Address: 10913 Huntcliff Drive, Apartment 9  
Owings Mills, MD

Race: Black/African American



**ATTACHMENT B-1**  
**LIST OF ITEMS TO BE SEIZED AND SEARCHED**

1. All records or other information located at the premises described in Attachments A1, A2, A4 and A5 related to the fruits, instrumentalities, and evidence of violations of Title 18, United States Code, Section 1344 (Bank Fraud) and Title 18, United States Code, Section 1343 (Wire Fraud) to include:

- a. Records, ledgers, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, money orders, bank drafts, wire transfers, letters of credit, cashier's checks, bank checks, safe deposit box keys, and other items which demonstrate the obtaining, secreting, transfer, expenditures(s) and/or concealment of assets and money; including any computerized or electronic records.
- b. United States and foreign currency, and financial instruments.
- c. Photographs, including still photos, negatives, video tapes, films, undeveloped film and the contents therein, to include photographs of monetary instruments, bank records, co-conspirators or assets.
- d. Address books and their contents reflecting names, addresses, and telephone numbers, including computerized or electronic records.
- e. Any locked or closed containers including but not limited to safes, both combination and lock type, and their contents.
- f. Any identification card or other means of identification which is authentic or fraudulent, including passports and/or state identification cards and applications for the same. Any equipment which could be used to produce fraudulent checks or other false identification information.
- g. Evidence of vehicles, devices, property or other items and services which represent purchases using stolen identities, financial instruments associated with fraud, or the proceeds of fraud or financial crimes.
- h. Digital devices used in the commission of, or to facilitate, the above-described offenses, including to communicate with co-conspirators and to store and transmit images and documents involved in the scheme, such as bank records and photos to be used to manufacture fraudulent identification documents.
- i. Clothing and clothing accessories (i.e. shirts, sunglasses, hats) that may be used to identify and attribute persons involved in the fraud schemes.
- j. Debit cards, credit cards, gift cards, or any other items in which fraudulently obtained funds could be loaded.

2. All images, messages, and communications regarding methods to avoid detection by law enforcement;

3. Any and all documents, records, or correspondence pertaining to occupancy, ownership or other connection to the following premises, which are described further in Attachments A1, A2, A3, and A4:

- a. 130 Persimmon Circle, Reisterstown, MD;
- b. 10913 Huntcliff Drive, Apartment 9, Owings Mills, MD;
- c. Apple iPhone X with International Mobile station Equipment Identity number (IMEI) 354876091091293; and
- d. A dark colored Toyota Corolla bearing a Maryland license plate 6BV6137.

4. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to the specified criminal offenses. The following definitions apply to the terms as set out in this affidavit and attachment:

a. Computer hardware: Computer hardware consists of all equipment, which can receive, capture, collect analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to cellular telephones, central processing units, laptops, tablets, eReaders, notes, iPads, and iPods; internal and peripheral storage devices such as external hard drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

b. Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

c. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a

string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touches. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

As used above, the terms “records, documents, messages, correspondence, data, and materials” includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

5. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, “COMPUTER”) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the Device(s);

- j. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- k. contextual information necessary to understand the evidence described in this attachment.

6. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

- a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- c. "scanning" storage areas to discover and possibly recover recently deleted files;
- d. "scanning" storage areas for deliberately hidden files; or
- e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of theft of government property or other criminal activity, the further search of that particular directory, file or storage area, shall cease.



**ATTACHMENT B-2**

**ITEMS TO BE SEIZED**

All records contained in the item described in Attachment A3 which constitute evidence of violations of 18 U.S.C. § 1344 (Bank Fraud) and 18 U.S.C. § 1343 (Wire Fraud) as outlined below:

1. All records, ledgers, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, money orders, bank drafts, wire transfers, letters of credit, cashier's checks, bank checks, safe deposit box keys, and other items which demonstrate the obtaining, secreting, transfer, expenditures(s) and/or concealment of assets and money; including any computerized or electronic records.
2. Photographs, including still photos, negatives, video tapes, films, undeveloped film and the contents therein, to include photographs of monetary instruments, bank records, co-conspirators or assets.
3. Address books and their contents reflecting names, addresses, telephone numbers; including computerized or electronic records.
4. Any data related to an identification card or other means of identification which is authentic or fraudulent, including passports and/or state identification cards and application for the same. Any data related to equipment which could be used to produce fraudulent checks or other false identification information.
5. Evidence of vehicles, devices, property or other items and services which represent purchases using stolen identities, financial instruments associated with fraud, or the proceeds of fraud or financial crimes.
6. Digital devices used in the commission of, or to facilitate, the above-described offenses, including to communicate with co-conspirators and to store and transmit images and documents involved in the scheme, such as bank records and photos to be used to manufacture fraudulent identification documents
7. Information related to debit cards, credit cards, gift cards, or any other items in which fraudulently obtained funds could be loaded.
8. All images, messages, and communications regarding methods to avoid detection by law enforcement;
9. Any and all information pertaining to occupancy, ownership or other connection to the following premises, which are described further in Attachments A1, A2, A3, and A4:
  - a. 130 Persimmon Circle, Reisterstown, MD;
  - b. 10913 Huntcliff Drive, Apartment 9, Owings Mills, MD;

- c. Apple iPhone X with International Mobile station Equipment Identity number (IMEI) 354876091091293; and
- d. A dark colored Toyota Corolla bearing a Maryland license plate 6BV6137.

10. Any and all records related to the location of the user(s) of the device.

11. For the Device:

- a. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;
- e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the Device;
- f. evidence of the times the Device were used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the Device;
- h. documentation and manuals that may be necessary to access the Device or to conduct a forensic examination of the Device;
- i. contextual information necessary to understand the evidence described in this attachment.

12. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like

those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

- a. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- b. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- c. “scanning” storage areas to discover and possibly recover recently deleted files;
- d. “scanning” storage areas for deliberately hidden files; or
- e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

13. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.